

# Section C - Description/Specifications/Statement of Work

## Statement of Work (SOW) for

### Code 225 Program Management Support and Associated System Engineering Service Support

#### 1.0 INTRODUCTION

1.0.1 The Naval Surface Warfare Center Philadelphia Division (NSWCPD) is a Department of Defense entity responsible for research and development, test and evaluation, engineering and fleet support organization for the Navy's ships, submarines, military watercraft and unmanned vehicles. This requirement is for NSWCPD Code 225, which is responsible for program management and associated system engineering services for NSWCPD's In-Service Ships & Cross Platform Engineering group.

1.0.2 This contract is for non-personal services. It does not create employment rights with the U.S. Government whether actual, inherent, or implied

1.0.3 Government / Contractor Relationship

a). The services to be delivered under this Task Order are non-personal services and the parties recognize and agree that no employer-employee relationship exists or will exist under the Task Order between the Government and the Contractor's personnel. Therefore, it is in the best interest of the Government to provide both parties a full understanding of their respective obligations.

b). The Contractor employees shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and displaying distinguishable badges or other visible identification for meetings with Government personnel. In addition, Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

c). Contractor personnel under this Task Order shall not engage in any of the inherently Governmental functions listed at FAR Subpart 7.5 or DFARS Subpart 207.5.

d). Employee Relationship:

- 1) The services to be performed under this Task Order do not require the Contractor or its personnel to exercise personal judgment and discretion on behalf of the Government. Rather the Contractor's personnel will act and exercise personal judgment and discretion on behalf of the Contractor.
- 2) Rules, regulations, directives, and requirements that are issued by the U. S. Navy and NSWCPD under its responsibility for good order, administration applicable to all personnel who enter a Government installation or who travel on Government transportation. This is not to be construed or interpreted as Government control that is inconsistent with a non-personal services contract.

e). Inapplicability of Employee Benefits: This Task Order does not create an employer-employee relationship. Accordingly, entitlements and benefits applicable to such relationships do not apply.

f). Notice. It is the Contractor's, as well as the Government's, responsibility to monitor Task Order activities and notify the Contracting Officer if the Contractor believes the intent of this Section has been or may be violated.

- 1) The Contractor shall notify the Contracting Officer in writing via letter or email within three (3) calendar days from the date of any incident that the Contractor constitute a violation of this Section. The notice should include the date, nature, and circumstances of the conduct; the name, function, and activity of the employee or Contractor official or employee involved or knowledgeable about such conduct; identify any documents or substance of any oral communication; and the Contractor's estimated date when, absent a response, cost, schedule or performance will be impacted.
- 2) The Contracting Officer will, within five (5) calendar days after receipt of notice, respond to the notice in writing. In responding, the Contracting Officer will:
  - (i) Confirm the conduct is in violation and when necessary direct the mode of further performance,
  - (ii) Countermand any communication regarded as a violation,
  - (iii) Deny that the conduct constitutes a violation and when necessary direct the mode of further performance, or
  - (iv) In the event the notice is inadequate to make a decision, advise the Contractor what additional information is required, and establish the date by which the Contractor must provide the information.

### 1.1 BACKGROUND

This statement of work is for Program Management support and associated system engineering services for NSWCPD's In-Service Ships & Cross Platform Engineering group, Code 225. Specific tasks will be associated with U.S. Navy ships and will include LPD 17 Class, LHD and LHA Classes, DDG 51 and CGs Classes, LSD 41 and 49 Classes, LCC 19, PC Class, MCM Class and SEA21 Sustainment Programs. Services described within this document will assist Code 225 in providing direct support to program offices such as NAVSEA SEA 21 (PMS 400, PMS 443, PMS 470), SEA 05, Fleet Type Commanders (TYCOMs) and Surface Maintenance Engineering Planning Program (SURFMEPP). The goal of this task order is to support and enhance existing programs and services within Code 225's cognizance.

The program management support tasks of this SOW include financial management support; coordination/scheduling of large projects and program-level engineering services for In-Service Ships & Cross Platform Engineering; and system engineering support of in-service taskings such as Ship Alterations (ShipAlts), Ship Change Documents (SCD), Authorized Work Items (AWI), repairs, system operability testing, system certification and inspections, Chief of Naval Operations availability planning and general modernization/sustainment management.

**NOTE: References to, and execution of any tasks regarding, "financial management" and "budgetary support", shall be limited to non-procurement sensitive information; upon discovery of any tasks where procurement-sensitive information is accessed, Contractor shall cease all activities related to the procurement-sensitive information and immediately report the discovery to the Procuring Contracting Officer and Contracting Officer's Representative.**

**"Procurement-sensitive information" as it relates to this SOW, is defined as information where the identity and/or economic/financial posture of prime and subcontractors which – if accessed - could unfairly damage the competitiveness of future procurements.**

### 1.2 SCOPE OF WORK

The Contractor shall support NSWCPD Program Management Support and Associated System Engineering efforts in the following areas:

- a. Program Management Support
- b. Program Support – Meeting Coordination Support
- c. Program Support – Database Support
- d. Program Support – System Engineering

## e. Program Support – Logistics

**2.0 APPLICABLE DOCUMENTS**

- 2.1 General Specifications for Overhaul of Surface Ships (GSO) - NAVSEA S9AA0-AB-GOS-010 (2016) [HTTPS://INAVY.PORTAL.NAVY.MIL/](https://INAVY.PORTAL.NAVY.MIL/)
- 2.2 NAVY MODERNIZATION PROCESS MANAGEMENT AND OPERATIONAL MANUAL (NMP-MOM), Rev 3 dated January 2010 <https://www.nde.navy.mil/>
- 2.3 Ship Alterations accomplished by AIT - NAVSEA Technical Specification 9090-310G, dated Feb 2015 <https://www.nde.navy.mil/>
- 2.4 MIL-STD-1689, Fabrication, Welding and Inspection of Ships Structure, Rev A, dated 23 Nov 1990 <https://login.ihserc.com/login/erc>
- 2.5 Manuals, Technical: General Style and Format of (work Package Concept) - MIL-DTL-81927C, dated 26 Nov 1997 <https://login.ihserc.com/login/erc>
- 2.6 Standard Practice for Manuals, Technical: General Style and Format - MIL-STD-38784A, dated 25 August 2011 <https://login.ihserc.com/login/erc>
- 2.7 Interactive Electronic Technical Manuals - MIL-DTL-87269D dated 30 January 2014, Data Base, Revisable <https://login.ihserc.com/login/erc>
- 2.8 Manuals, Technical, General Acquisition and Development Requirements - MIL-DTL-24784, Rev C, dated 03 Nov 2007 <https://login.ihserc.com/login/erc>
- 2.9 Technical Manual Users Quick Reference Guide- S0005-AG-GYD-010 Rev 01 <https://mercury.tdmis.navy.mil>
- 2.10 NAVSEA TECHNICAL MANUAL MANAGEMENT PROGRAM- S0005-AA-PRO-010/TMMP Rev 3 <https://mercury.tdmis.navy.mil>
- 2.11 MIL-HNBK-454B, General Guidelines for Electronic Equipment, dated 15 APR 2007 <http://www.dscclia.mil>
- 2.12 NAVSEA Standard Items (FY19 and future revisions) <http://www.navsea.navy.mil>
- 2.13 Tag Out User's Manual of NAVSEA Technical Manuals – S0400-AD-URM-010, Rev 7, dated 21 Nov 2013. <https://mercury.tdmis.navy.mil>
- 2.14 NAVSEA Fleet Modernization Program (FMP) Management and Operations Manual SI-720-0AA-MAN-010/202 <https://navsea.portal.navy.mil/Pages/default.aspx>
- 2.15 NAVSEA Engineering and Technical Authority Manual (ETAM) S9800-AB-MAN-010, dated 03 June 2011 [https://navsea.navy.deps.mil/field/cnrmc-marmc/200/DDL/S9800-AB-MAN-010\\_-\\_pdf#search=etam](https://navsea.navy.deps.mil/field/cnrmc-marmc/200/DDL/S9800-AB-MAN-010_-_pdf#search=etam)
- 2.16 DoD 8570.01-M "Information Assurance Workforce Improvement Program"
- 2.17 DoD 8140.01 "Cyberspace Workforce Management requirement"

The Contractor shall reference and utilize the latest version available when performing tasks within this SOW.

**3.0. REQUIREMENTS** - Contractor shall be excluded from accessing any procurement-sensitive information while performing tasks in this SOW. Should Contractor gain access to procurement-sensitive information, Contractor shall immediately report the findings to the Procuring Contracting Officer and Contracting Officer's Representative.

**3.1 Program Management Support**

3.1.1 NSWCPD Code 225 executes financial-program-management for surface ship modernization and sustainment of In-Service Programs. To support these activities, Contractor shall adhere to current funding rules/regulation as it executes the required support tasks. Contractor shall be able to receive database-downloads (i.e. ERP, NAVSEA Enterprise Planning System (NEPS), Confluence, and local shared drives and Task Planning Sheets (TPS) and project proposals) from NSWCPD in a Microsoft Excel format, and shall:

3.1.1.1 Analyze detailed financial information from databases, and provide a trend analysis;

3.1.1.2 Analyze the data weekly, and provide a report within two business days in accordance with (IAW) CDRL A006.

3.1.1.3 Analyze the data based on ad hoc direction of NSWCPD Code 225, and provide the findings IAW CDRL A006.

3.1.1.4 Support a weekly face-to-face meeting, as necessary, with NSWCPD Code 225 POC to review the programs under management.

3.1.2 Attend programmatic meetings to answer program/project-specific financial management and tracking related questions; more formal meetings shall require preparation and planning to ready comprehensive responses to NSWCPD management to be delivered by the appropriate support-contractor-personnel. It is anticipated that approximately six "formal" meetings will be held each year.

3.1.3. Support budget preparation - This consists of compiling task and project information for out years, with critical information driven by databases (i.e. ERP, NEPS, Confluence, and local shared drives and TPSs). Contractor shall assist NSWCPD with gathering, assembling, and forecasting budget-information regarding specific projects for NSWCPD-review. Task includes assistance with preparing briefs, and development of metrics to track actions, minutes, and milestones.

3.1.4. Sustainment and Modernization Support - Contractor shall implement system engineering processes, aligned with the Navy's overall methods of executing and maintaining surface ships to meet their expected service lives (sustainment and modernization), and receive and analyze detailed tasking information from databases (i.e. ERP, NEPS, Confluence, and local shared drives and TPSs) and other program and project management tools. NSWCPD Code 225 shall provide these efforts/reports, as well as specific criteria for analysis. Contractor shall:

3.1.4.1 Develop and provide redline and recommendations to increase efficiencies.

3.1.4.2 Develop and maintain detailed schedules in Microsoft Project and other associated software to analyze and project program and project tasking.

3.1.4.3 Integrate schedules with workload planning and multi-level milestones (Milestones such as CNO availabilities, Fiscal Year (FY) turnovers, Systems Engineering Plan (SEP), test and evaluations, Risk Management Framework (RMF))

3.1.4.3.1 Scheduling shall include the elements to support system integration, management of complex engineering efforts, qualification and certification process, workload analysis and various programmatic milestones. Schedules shall:

3.1.4.3.1.1 Be maintained and updated monthly

3.1.4.3.1.2 Be tracked by program within Code 225

3.1.4.3.2 Utilize information from resources such as NAVSEA Data Environment (NDE) modernization, databases (i.e. ERP, NEPS, Confluence, local shared drives, and TPSs), program reviews, System Health Assessments (SHA) and Class Management Teams (CMT) data, white paper, ERP financial data and fleet schedules to compile and analyze schedules

3.1.5 Tracking Support - Contractor shall assist with sustainment task tracking and management; tasks include:

3.1.5.1 NDE and SCD Tracking - Contractor shall assist with the NAVSEA Data Environment (NDE) and SCD tracking at both a project level and program level. This can include both fleet and program efforts associated with HM&E equipment. Contractor shall analyze information based on direction of NSWCPD Code 225, and report findings and recommendations; requests for analysis may include reviews of:

3.1.5.2 Method of installations

3.1.5.3 Hull applicability

3.1.5.4 Installations schedules and differences in task planning documents

3.1.5.5 Scheduled modernization milestones, to include recommendations for the inclusion of new events

3.1.5.6 Coordination, task validation, and communication with ISEAs/SMEs within NSWCPD for status and report develop.

3.1.5.7 Monitor, track, update, and coordinate task deliverables to ensure the most accurate information is available upon request.

3.1.6 SCD Support - Contractor shall initiate and draft SCD documents IAW of In-Service Engineering Agents (ISEAs) for their review. Contractor shall:

3.1.6.1 Utilize the NDE/SCD Entitlement database to reference information and to create documents.

3.1.6.2 Capture, integrate, and develop SCDs based on information from NSWCPD's ISEAs; information such as hull applicability, technical and change summary, Integrated Logistics System (ILS) impacts, qualification, fielding and cost estimating information critical to SCD initiation shall be incorporated and managed/updated with new developments. The intent of this task is not to be a detailed engineering effort, rather a programmatic and system integration management focused effort.

3.1.7 NDE/SCD Entitlement Review Process - Contractor shall assist with managing and coordinating the NDE/SCD Entitlement Review Process; this includes applying knowledge of the Technical Assessment Team (TAT) review process to support submissions and responding to findings in a timely manner; responses may only require coordination or the actual data entry (Or a mix of the two methods).

3.1.8 System Health Assessments (SHA) and Class Management Teams (CMT) Support – Contractor shall assist with the development, tracking and execution of the annual SHA development; this task requires coordination, analysis, and preparation-support to the ISEAs with database submissions (this includes all steps of this process) to include any necessary follow-on reviews and updates. (Associated database is discussed later in this document at Section 3.3.1)

3.1.9 Program Risk Support (Note: This is different from System Engineering Risk Support stated at Section 3.4.1) – Contractor shall:

3.1.9.1 Identify, assess, and recommend solutions to mitigate risks to acceptable level; Contractor shall create, coordinate, and manage identified program risks and report upon them, as necessary.

3.1.9.2 Report upon the HM&E shipboard equipment and systems for the assigned ship classes.

3.1.9.3 Include information regarding risk on the various stages of the system and/or the overall program.

3.1.9.4 Include the identification and validation of probabilities and severities.

3.1.9.5 Contractor shall be required to analyze the data based on direction of NSWCPD Code 225 (to limit scope to pertinent subjects).

3.1.10 Associated with the above taskings Contractor shall report on the following:

3.1.10.1 Financial report detailing the programs' required, allocated, obligated, and expended funding (CDRL A006)

3.1.10.2 Status reporting detailing the program execution (CDRL A001)

3.1.10.3 Meeting minutes of weekly, monthly or quarterly program meetings including tracking of action items (CDRL A001)

**3.2 Program Support – Meeting Coordination/Support** – As part of its program management of programs/projects, Code 225 frequently hosts, as well as participates, in various meetings involving numerous stakeholders. Code 225 requires support for these activities. Meetings will likely discuss Distro D-level information. Locations are likely to be Philadelphia, PA Naval Business Center, Washington, DC, San Diego, CA and Norfolk/Virginia Beach, VA. Typical meetings include annual reviews, quarterly program reviews and other program/technical-based meetings. 50 annual meetings are projected; approximate number of attendees is 20; attendees will likely possess a DoD Security clearance; of the 50 meetings, 10 will require support for a larger audience than 20 (approximately 100) and can range from a few hours to multiple days. Contractor shall:

3.2.1 Prepare rooms with screens, projectors, whiteboards, audio/telecom capabilities and seating arrangements in accordance with NSWCPD protocol and requirements.

3.2.2 Assist with agenda development and tracking of the attendee invites/lists.

3.2.3 Support Non-government and Government Conference Room Spaces, or government supplied spaces, as appropriate.

3.2.4 Ensure hard and soft copies of materials, as necessary, are available to attendees; this shall include the development of graphics, poster displays, pamphlets, agenda, tent cards, CD-ROMS, and booklet/binders (Typically, soft copies shall be provided 3-5 business days prior).

**3.3 Program Support – Database Support** - Code 225 plans to continue to manage and support the System Health Assessment (Access Database), as well as to develop and maintain a web application by integrating it into the Code 1042 Philadelphia Division Intranet (PDI) web site. To support these activities, Contractor shall:

3.3.1 Analyze the PDI web application, and model a front-end and back-end architecture to this standard; support shall include:

3.3.1.1 Converting all existing front-end functionality of SHA Access Database into a web application.

3.3.1.2 Converting all existing back-end functionality of SHA Access Database into an Oracle database.

3.3.1.3 Provide documentation of all requirements IAW NSWCPD SEP.

3.3.1.4 Perform Developmental and Operational Testing.

3.3.2 Leverage expertise with Microsoft Office Suite (including Excel, PowerPoint, Project and Access) to develop macros and tools to analyze and maintain data for programmatic needs; efforts include work with large data sets that will be integrated into different management tools, databases and reports.

3.3.3 Deliver Computer Software Product IAW CDRL A007 for all developed applications.

#### **3.4 Program Support – System Engineering**

**3.4.1 Risk/System Engineering** - Contractor shall implement risk/system engineering processes and comply with the Navy's overall methods of executing and maintaining surface ships to help meet their expected service life (i.e. Sustainment and Modernization). Contractor shall:

3.4.1.1 Assist with system inspections by identifying hazards for known issues.

3.4.1.2 Analyze identified hazards from a system-safety and reliability point of view.

3.4.1.3 Conduct system and/or component failure/root cause analysis.

3.4.1.4 Conduct system reliability analysis.

3.4.1.5 Conduct system failure modes analysis.

3.4.1.6 Generate conceptual design proposals, consisting of both engineering studies and sketches, for NSWCPD review.

3.4.1.7 Perform feasibility studies for conceptual design proposals.

3.4.1.8 Support NSWCPD adhere to DoD's system engineering process.

3.4.1.9 Assist NSWCPD with implementation of proposed design requirements for conversions, overhauls, alterations, modifications and installations.

3.4.1.10 Provide the results of the analysis, feasibility studies, and tests in accordance with CDRL A008

**3.4.2 Cyber-secure System Support** – Contractor shall assist with the development and submission of Risk Management Framework risk assessments; implement DoD secure system configuration and hardening requirements from Defense Information System Agency, Security Technical Implementation Guides and Security Guides; conduct Assured Compliance Assessment Solution vulnerability assessments, anti-virus scanning, and produce System Engineering Process artifacts, as necessary.

#### **3.4.3 Engineering Support**

**3.4.3.1 On-site Engineering and Technical Services Support** - During construction, Combat Support Systems Onboard Testing (CSSOT), in-service, and maintenance periods in connection with the installation, maintenance or alteration of Surface Ship (primarily Surface Combatants) Hull, Mechanical and Electrical (HM&E) Combat Support Systems and components, Contractor shall ensure equipment tests are conducted/completed in accordance with test procedures and/or work packages. Contractor shall provide equipment status/problems, along with recommendations for solutions. The majority of this support will be at Surface Ship Homeports and Building Yards.

3.4.3.2 Contractor shall investigate and review HM&E/Combat Support Systems equipment, Work Packages for Post Shakedown Availabilities (PSA), Post Delivery

Availabilities (PDA), Selected Restricted Availabilities, (SRA) and Dry-dock Selected Restrictive Availabilities (DSRA) to ensure correct technical content, priority, category, and applicability. Ship systems will include main propulsion, auxiliary machinery, interior and exterior paint, decking and corrosion control. Contractor shall track Work Packages and monitor work progress status on a daily basis on-site at Ship's location. Contractor shall:

3.4.3.2.1 Witness the installation of ship and machinery alterations and report deviations from planned execution; witness field tests of ship systems and equipment evaluate/document their performance as compared to detailed design parameters; assist with technical resolution of installation issues, material issues, and implementation corrective actions.

3.4.3.2.2 Provide engineering, technical and repair support to accomplish assignments in support of conversions, overhauls, alterations, modifications, installations, repair and removal of shipboard equipment and associated systems installed equipment on USN and MSC ships.

3.4.3.2.3 Develop Waterfront Plan of Action and Milestones (POA&M) in Microsoft Project for NSWCPD's review.

3.4.3.2.4 Assist with configuration management of program data including the tracking of Engineering Change Proposals.

3.4.3.2.5 Support implementation of fleet maintenance philosophies, as well as Integrated Logistic Support (ILS) procedures and functions of the Ship's Logistics Support Center (LSC)/Maintenance Support Center (MSC).

3.4.3.2.6 Support Naval Surface Warfare Center Philadelphia Division's (NSWCPD) role as HM&E In-service Agent and efforts to ensure system compatibility for all equipment; Contractor shall help determine/configure proper interface requirements, verify specifications, and assist with the development of long-term maintenance/upgrade strategies.

3.4.3.3 Provide the results of the tests and analysis in accordance with CDRL A008.

### **3.5 Program Support – Logistics**

3.5.1 Integration of ILS products – Contractor shall assist NSWCPD with forecasting material needs, and providing metrics that communicate current levels of readiness and sustainment pertaining to maintenance, utilizing information from the Fleet (TYCOM, RMC) and SYSCOM (NAVSEA, SURFMEPP). Contractor shall provide technical analysis, recommendations, white papers, and other documents for logistics-issues related to ILS life-cycle support regarding sparing, support equipment requirements, advanced planning, and work package development

3.5.2 Ship Availabilities - Contractor shall identify, characterize, track and monitor logistics milestones for Ship Availabilities. Contractor shall provide status and Ship Availability planning updates to appropriate stakeholders and their organizations. Contractor shall review Ship Change Documents (SCDs) for ILS impacts to readiness/sustainment and update, verify and process Technical Manuals, PMS, Provisioning, Training, EOSS, Configuration and ILS Certifications, as well as provide recommendations to close gaps/deficiencies identified; recommend actions to correct deficiencies and assist in reviewing Coordinated Shipboard Allowance Lists (COSAL); participate in Advanced Planning and ILS Working Groups.

3.5.3 Contractor shall track HM&E equipment related class and ISEA advisories for U.S. Navy and FMS auxiliary, combatant, amphibious and minesweeping ships. Contractor shall assist in issuing, updating, and closing advisories, and provide a tracking matrix detailing the status of all advisories.

### **3.6 Commonality of Systems, Subsystems, and Components**

Not applicable

### **3.7 Manufacturing Phase-Out or Discontinuation of Production, Diminishing Sources, and Obsolete Materials or Components**

3.7.1 The contractor shall notify the contracting officer immediately upon determining the unavailability of obsolete materials or components. The contractor may recommend a solution to include the impact on the contract price and delivery. The contractor shall not initiate any item redesign or incur any additional costs without the express, written authorization of the contracting officer.

### **3.8 Diminishing Manufacturing Sources and Material Shortages Management (DMSMS) Contract Requirements**

Not applicable

### **3.9 Parts Obsolescence**

Not applicable

**4.0 DATA REQUIREMENTS** - The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is

required from the COR.

#### **4.1 Contract Status Report (CDRL A001)**

- 4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.
- 4.1.2 The Government's approval must be received in writing from the COR within 5 business days before formal submission.
- 4.1.3 This report is applicable to all activities within Section 3.0.

#### **4.2 Travel Report (CDRL A002)**

- 4.2.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

#### **4.3 Contractor's Personnel Roster (CDRL A003)**

#### **4.4 Small Business Utilization Report (CDRL A004)**

- 4.4.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

#### **4.5 Systems Security Plan CDRL (A005)**

- 4.5.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

#### **4.6 Funds Status Report (CDRL A006)**

4.6.1 There may be a need for tailoring beyond the specifications in this CDRL; should that be the case, the report format, contents and delivery requirements will be specified at the time of Technical Instruction (TI) issuance.

#### **4.7 Computer Software Product (CDRL A007)**

#### **4.8 Technical Report - Study/Services (CDRL A008)**

4.8.1 There may be a need for tailoring beyond the specifications in this CDRL; should that be the case, the report format, contents and delivery requirements will be specified at the time of Technical Instruction (TI) issuance.

### **5.0 SECURITY REQUIREMENTS**

5.1 The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; NAVSEA Physical Security training and Cybersecurity 101 Training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.2 In accordance with SECNAV M-5510.30 Chapters 5 and 6, all Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site are designated Non-Critical Sensitive/IT-II positions, which require an open investigation or favorable adjudicated National Agency Check (NACLC) by the Defense Counterintelligence and Security Agency (DCSA). Investigations should be completed using the SF-86 Form and the SF-87 finger print card. An interim clearance can be granted by the company Security Officer and recorded in the Defense Information System for Security (DISS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD sites and buildings. If an unfavorable adjudication is determined by DCSA all access will be terminated. For Common Access Card (CAC) card you must have a completed investigation that has been favorably adjudicated or a final security clearance. A CAC Card will not be issued to contractors who have an interim security clearance.

5.3 Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

5.4 Construction badges for contractor personnel that work on-site at one of the NSWCPD sites will be good for 60 days.

5.5 A Facility Access Determination (FAD) will be completed on any contractor that does not have a favorable adjudicated investigation in DISS and is requesting swipe/non-swipe access to our buildings in excess of 120 days. Any contractor that has unfavorable information that has not been favorably adjudicated by Department of Defense Central Adjudication Facility (DOD CAF) will not be issued a badge.

5.6 This effort may require access to classified information up to the SECRET level. No classified data will be generated or stored by the Contractor. The requirements of the attached DD Form 254 apply. An Active SECRET Facility Clearance (FCL) is required for performance on this contract. All contractor personnel accessing classified information or classified material associated with the performance work relative to the resultant contract must be United States citizens and shall have and maintain SECRET security clearance at time of contract award. Interim clearance is acceptable. All classified data and hardware will be protected IAW 37 CFR Part 117, National Industrial Security Program Operating Manual (NISPOM). The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWC Philadelphia Division's (NSWCPD) Critical Information List will be provided on site, if warranted.

5.6.1 Performance under this contract requires the contractor to adhere to OPSEC requirements. The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements.

5.6.2 During the period of this contract, the Contractor may be exposed to, use, or produce, NSWC PD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI). CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be protected per NIST SP-800- 171, Protecting Controlled Unclassified Information in Non-federal Systems and Organizations. Assembled large

components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible. NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites.

5.6.3 Media requests related to this project shall be directed to NSWCPD Public Release Authority listed in Item 12 of the DD Form 254. Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWCPD Security Division (Code

1051). Questions concerning these requirements shall be directed to the NSWCPD Security Division (Code 1051).

- The Contractor must submit a request for sharing of classified and other sensitive information between prime contracts in writing to the Security Office, Code 1051 identified in Item 17 of this form.

- All classified information involved in security incidents shall be retained and provided to the certifying official in Item 17 of this DD 254 for classification review.

- All Controlled Unclassified Information (CUI) associated with this contract must be safeguarded to prevent unauthorized public disclosure. CUI such as FOUO, Security Classification Guides (SCG), and other technical information with Distribution Statements B, C, D, E or F are not authorized for public release and cannot be placed on a publicly accessible web site or web server. All emails containing such information or attachments, shall be protected per NIST SP-800-171. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast,

etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy all CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

5.7 The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (IAW 37 CFR Part 117), and (3) assure compliance with any written instructions from the NSWCPD, Security Office.

5.8 The Prime Contractor shall:

5.8.1 Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.

5.8.2 Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.

5.8.3 Submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

#### **5.9 Contractor shall comply with the following requirements as stated within the DD254:**

An Active SECRET Facility Clearance (FCL) is required for performance on this contract. There are no safeguarding requirements required.

All contractor-personnel accessing classified information or material associated with and/or performing work relative to the resultant contract must be United States citizens and shall have and maintain at a minimum a final SECRET security clearance at time of contract award.

-Item 10(j) 11(l): DoD M-5200.01 Volume 4, DoD Information Security Program: Controlled Unclassified Information (CUI) of 2/24/2012.

-Item 11(e), Engineering Services: This contract is for engineering services at the NSWC Philadelphia Division System, Philadelphia and/or its associated cleared facilities. Classification markings on the material to be furnished will provide the classification guidance necessary for performance of this contract.

Classified or unclassified technical papers to be presented at a classified symposium must be approved by the NSWCPD Contracting Officer's Representative (COR) prior to the presentation.

-Security classification guides and controlled unclassified information(CUI) (e.g., FOUO, distribution statement controlled) are not authorized for public release; therefore, they cannot be posted on a publicly accessible web-server or transmitted over the internet unless appropriately encrypted. Request for public release cannot be transmitted via the internet until the contractor receives final approval from NSWCPD (Code 1051).

-Contractor must submit a request for sharing of classified and other sensitive information between prime contracts in writing to the NSWCPD (Code 1051) identified in Item 17 of this form.

-Personnel designated as derivative classifiers shall receive derivative classification training prior to access from the contractor's Facility Security Officer (FSO). The FSO shall ensure personnel receive initial and biennial training during the life of this contract. Evidence of completion, training certificates or equivalent, shall be provided to the Information Assurance Manager no later than the individual's due date.

-All classified documents must be destroyed using a National Security Agency (NSA) approved high security crosscut shredder listed on the NSA/CSS evaluated products list(EPL) for high security crosscut paper shredders, or other approved method for destroying classified information.

-All classified information involved in security incidents shall be retained and provided to the certifying official in Item 17 of this DD 254 for classification review.

-All reports of contractor security violations associated with this contract shall be sent by the Cognizant DSS field office directly to the certifying official in Item 17 of this DD254.

-Forward a copy of subcontractor DD 254s issued under this contract to the official shown in item 17 of this DD254.

-All security related requests pertaining to this contract shall be submitted in writing by the contractor's Facility Security Officer (FSO) to the individual identified in Item 17 of this DD254.

-Classified or unclassified technical papers to be presented at a classified symposium must be approved by the NSWCPD Contracting Officer's Representative (COR) prior to the presentation.

-Security classification guides and controlled unclassified information(CUI) (e.g., FOUO, distribution statement controlled) are not authorized for public release; therefore, they cannot be posted on a publicly accessible web-server or transmitted over the internet unless appropriately encrypted. Request for public release cannot be transmitted via the internet until the contractor receives final approval from NSWCPD (Code 1051).

-Contractor must submit a request for sharing of classified and other sensitive information between prime contracts in writing to the NSWCPD (Code 1051) identified in Item



17 of this form.

-Personnel designated as derivative classifiers shall receive derivative classification training prior to access from the contractor's Facility Security Officer (FSO). The FSO shall ensure personnel receive initial and biennial training during the life of this contract. Evidence of completion, training certificates or equivalent, shall be provided to the Information Assurance Manager no later than the individual's due date.

-All classified documents must be destroyed using a National Security Agency (NSA) approved high security crosscut shredder listed on the NSA/CSS evaluated products list(EPL) for high security crosscut paper shredders, or other approved method for destroying classified information.

-All classified information involved in security incidents shall be retained and provided to the certifying official in Item 17 of this DD 254 for classification review.

-All reports of contractor security violations associated with this contract shall be sent by the Cognizant DSS field office directly to the certifying official in Item 17 of this DD254.

-Forward a copy of subcontractor DD 254s issued under this contract to the official shown in item 17 of this DD254.

-All security related requests pertaining to this contract shall be submitted in writing by the contractor's Facility Security Officer (FSO) to the individual identified in Item 17 of this DD254

**Additional information related to the facility clearance process can be obtained by visiting [www.dss.mil](http://www.dss.mil) or [http://www.dss.mil/isec/pcl\\_index.htm](http://www.dss.mil/isec/pcl_index.htm).**

#### **5.10 U-NNPI SECURITY REQUIREMENTS** (Ensure this section matches Security Office's input )

**5.10.1** Security Classification Guidance is as follows of portions of the tasking on this contract when invoked in the task order statement of work:

**5.10.1.1** Contractor requires access to information and equipment classified at the Confidential National Security Information (NSI) level in order to provide industrial support services within facilities that actively supports the Navy Nuclear Propulsion Program (NNPP).

**5.10.1.2** All contractor personnel accessing classified information or classified material associated with the performance of work related to the resultant contract must be United States citizens, and shall have and maintain at a minimum Confidential security clearance.

**5.10.1.3** The Contractor is responsible for completing all required government mandated training to maintain security and network access to government sites and IT systems, as necessary to support.

#### **5.11 U-NNPI**

**5.11.1** Purpose The Contractor hereby agrees that when provided documents (specifications, drawings, etc.) that are marked as containing NOFORN sensitive information that must be controlled pursuant to Federal law, the information contained therein and generated as part of the inquiry shall be used only for the purpose stated in the contract and shall in no case be transmitted outside the company (unless such transmittals comply with the detailed guidance of the contract) or to any foreign national within the company. While in use, the documents shall be protected from unauthorized observation and shall be kept secure so as to preclude access by anyone not having a legitimate need to view them. The documents shall not be copied unless done in conformance with the detailed guidance of the contract. All the documents shall be promptly returned in their entirety, unless authorized for proper disposal or retention, following completion of the contract.

#### **5.12.2 Specific Requirements for Protecting U-NNPI**

- a) Only U.S. citizens who have a need to know required to execute the contract shall be allowed access to U-NNPI.
- b) When not in direct control of an authorized individual, U-NNPI must be secured in a locked container (e.g., file cabinet, desk, safe). Access to the container must be such that only authorized persons can access it, and compromise of the container would be obvious at sight. Containers should have no labels that indicate the contents. If removed from the site, U-NNPI must remain in the personal possession of the individual. At no time should U-NNPI be left unsecured (e.g., in a home or automobile, or unattended in a motel room or sent with baggage).
- c) U-NNPI documents will have the word NOFORN at the top and bottom of each page. The cover sheet will have the warning statement shown below. Documents originated in the course of work that reproduce, expand or modify marked information shall be marked and controlled in the same way as the original. Media such as video tapes, disks, etc., must be marked and controlled similar to the markings on the original information.
- d) U-NNPI may not be processed on networked computers with outside access unless approved by CNO (N00N). If desired, the company may submit a proposal for processing NNPI on company computer systems. Personally owned computing systems, such as personal computers, laptops, personal digital assistants, and other portable electronic devices are not authorized for processing NNPI. Exceptions require the specific approval of the cognizant DAA and CNO (N00N).
- e) U-NNPI may be faxed within the continental United States and Hawaii provided there is an authorized individual waiting to receive the document and properly control it. U-NNPI may not be faxed to facilities outside the continental United States, including military installations, unless encrypted by means approved by CNO (N00N).
- f) U-NNPI may be sent within the continental United States and Hawaii via first class mail in a single opaque envelope that has no markings indicating the nature of the contents.
- g) Documents containing U-NNPI shall be disposed of as classified material.
- h) Report any attempts to elicit U-NNPI by unauthorized persons to the appropriate security personnel.
- i) Report any compromises of U-NNPI to the appropriate security personnel. This includes intentional or unintentional public release via such methods as theft, improper disposal (e.g., material not shredded, disks lost), placement on Web site, transmission via email, or violation of the information system containing U-NNPI.
- j) The only approved storage for U-NNPI is CDMS NOFORN.

#### **5.13.1 OPERATIONS SECURITY (OPSEC)**

**5.13.1.1** The Contractor shall protect critical information associated with this contract to prevent unauthorized disclosure. The NSWC Philadelphia Division's (NSWCPD) Critical Information List (CIL)/ CIIL (Critical Indicators and information list) will be provided on site, if warranted. Performance under this contract requires the contractor to adhere to OPSEC requirements. The Contractor may not impose OPSEC requirements on its subcontractors unless NSWCPD approves the OPSEC requirements. During the period of this contract, the Contractor may be exposed to, use, or produce, NSWCPD Critical Information (CI) and/or observables and indicators which may lead to discovery of CI. NSWCPD's CI will not be distributed to unauthorized third parties, including foreign governments, or companies under Foreign Ownership, Control, or Influence (FOCI).

**5.13.1.2** CUI correspondence transmitted internally on the contractor's unclassified networks or information systems, and externally, shall be

protected per NIST SP-800-171, Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations.

Assembled large components/systems being transported to and from testing areas, other production or government facilities (whether or not on public roadways) shall be in an enclosed van trailer or covered flatbed trailer. Component/System outside storage, staging, and test areas shall be shielded/obscured from public view wherever physically possible.

**5.13.1.3** NSWCPD's CI shall not be publicized in corporate wide newsletters, trade magazines, displays, intranet pages or public facing websites. Media requests related to this project shall be directed to the PCO, and the COR who will forward the required to the NSWCPD Public Release Authority for review.

**5.13.1.4** Any attempt by unauthorized third parties to solicit, obtain, photograph, or record, or; incidents of loss/compromise of government Classified or CI, Business Sensitive, Company Proprietary information related to this or other program must be immediately reported to the contractor's Facility Security Officer and Cognizant Security Office and/or the Naval Criminal Investigative Service, and the NSWC PD Security Division (Code 105.1). Questions concerning these requirements shall be directed to the PCO, and the COR who will forward the request to the NSWC PD Security Division (Code 105.1).

**5.13.2 RECEIPT, STORAGE, AND GENERATION OF CONTROLLED UNCLASSIFIED INFORMATION (CUI)** All Controlled Unclassified Information (CUI) associated with this contract must follow the minimum marking requirements of DoDI 5200.48, Section 3, paragraph 3.4.a, and include the acronym "CUI" in the banner and footer of the document. In accordance with DoDI 5200.48, CUI must be safeguarded to prevent Unauthorized Disclosure (UD). CUI export controlled technical information or other scientific, technical, and engineering information must be marked with an export control warning as directed in DoDI 5230.24, DoDD 5230.25, and Part 250 of Title 32, CFR. Nonfederal information systems storing and processing CUI shall be protected per NIST SP-800-171, or subsequent revisions. All transmissions to personal email accounts (AOL, Yahoo, Hotmail, Comcast, etc.) and posting on social media websites (Facebook, Instagram, Twitter, LinkedIn, etc.) are prohibited. Destroy CUI associated with this contract by any of the following approved methods: A cross-cut shredder; a certified commercial destruction vendor; a central destruction facility; incineration; chemical decomposition; pulverizing, disintegration; or methods approved for classified destruction.

**5.14** The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

## **5.15 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING**

### **5.15.1 System Security Plan and Plans of Action and Milestones (SSP/POAM) Reviews**

**5.15.1.1** Within thirty (30) days of contract award, the Contractor shall make its System Security Plan(s) (SSP(s)) for its covered contractor information system(s) available for review by the Government at the contractor's facility. The SSP(s) shall implement the security requirements in Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, which is included in this contract. The Contractor shall fully cooperate in the Government's review of the SSPs at the Contractor's facility.

**5.15.1.2** If the Government determines that the SSP(s) does not adequately implement the requirements of DFARS clause 252.204-7012 then the Government shall notify the Contractor of each identified deficiency. The Contractor shall correct any identified deficiencies within thirty (30) days of notification by the Government. The contracting officer may provide for a correction period longer than thirty (30) days and, in such a case, may require the Contractor to submit a plan of action and milestones (POAM) for the correction of the identified deficiencies. The Contractor shall immediately notify the contracting officer of any failure or anticipated failure to meet a milestone in such a POAM.

**5.15.1.3** Upon the conclusion of the correction period, the Government may conduct a follow-on review of the SSP(s) at the Contractor's facilities. The Government may continue to conduct follow-on reviews until the Government determines that the Contractor has corrected all identified deficiencies in the SSP(s).

**5.15.1.4** The Government may, in its sole discretion, conduct subsequent reviews at the Contractor's site to verify the information in the SSP(s). The Government will conduct such reviews at least every three (3) years (measured from the date of contract award) and may conduct such reviews at any time upon thirty (30) days' notice to the Contractor.

### **5.15.2 Compliance to NIST 800-171**

**5.15.2.1** The Contractor shall fully implement the CUI Security Requirements (Requirements) and associated Relevant Security Controls (Controls) in NIST Special Publication 800-171 (Rev. 1) (NIST SP 800-171), or establish a SSP(s) and POA&Ms that varies from NIST 800-171 only in accordance with DFARS clause 252.204-7012(b)(2), for all covered contractor information systems affecting this contract.

**5.15.2.2** Notwithstanding the allowance for such variation, the contractor shall identify in any SSP and POA&M their plans to implement the following, at a minimum:

**5.15.2.3** Implement Control 3.5.3 (Multi-factor authentication). This means that multi-factor authentication is required for all users, privileged and unprivileged accounts that log into a network. In other words, any system that is not standalone should be required to utilize acceptable multi-factor authentication. For legacy systems and systems that cannot support this requirement, such as CNC equipment, etc., a combination of physical and logical protections acceptable to the Government may be substituted;

**5.15.2.4** Implement Control 3.1.5 (least privilege) and associated Controls, and identify practices that the contractor implements to restrict the unnecessary sharing with, or flow of, covered defense information to its subcontractors, suppliers, or vendors based on need-to-know principles;

**5.15.2.5** Implement Control 3.1.12 (monitoring and control remote access sessions) - Require monitoring and controlling of remote access sessions and include mechanisms to audit the sessions and methods.

**5.15.2.6** Audit user privileges on at least an annual basis;

**5.15.2.7** Implement:

5.15.2.7.1 Control 3.13.11 (FIPS 140-2 validated cryptography or implementation of NSA or NIST approved algorithms (i.e. FIPS 140-2 Annex A: AES or Triple DES) or compensating controls as documented in a SSP and POAM); and,

5.15.2.7.2 NIST Cryptographic Algorithm Validation Program (CAVP) (see <https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program>);

5.15.2.8 Implement Control 3.13.16 (Protect the confidentiality of CUI at rest) or provide a POAM for implementation which shall be evaluated by the Navy for risk acceptance.

5.15.2.9 Implement Control 3.1.19 (encrypt CUI on mobile devices) or provide a plan of action for implementation which can be evaluated by the Government Program Manager for risk to the program.

### 5.15.3 Cyber Incident Response:

5.15.3.1 The Contractor shall, within fifteen (15) days of discovering the cyber incident (inclusive of the 72-hour reporting period), deliver all data used in performance of the contract that the Contractor determines is impacted by the incident and begin assessment of potential warfighter/program impact.

5.15.3.2 Incident data shall be delivered in accordance with the Department of Defense Cyber Crimes Center (DC3) Instructions for Submitting Media available at [http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions\\_for\\_Submitting\\_Media.docx](http://www.acq.osd.mil/dpap/dars/pgi/docs/Instructions_for_Submitting_Media.docx). In delivery of the incident data, the Contractor shall, to the extent practical, remove contractor-owned information from Government covered defense information.

5.15.3.3 If the Contractor subsequently identifies any such data not previously delivered to DC3, then the Contractor shall immediately notify the contracting officer in writing and shall deliver the incident data within ten (10) days of identification. In such a case, the Contractor may request a delivery date later than ten (10) days after identification. The contracting officer will approve or disapprove the request after coordination with DC3.

### 5.15.4 Naval Criminal Investigative Service (NCIS) Outreach

The Contractor shall engage with NCIS industry outreach efforts and consider recommendations for hardening of covered contractor information systems affecting DON programs and technologies.

### 5.15.5 NCIS/Industry Monitoring

5.15.5.1 In the event of a cyber incident or at any time the Government has indication of a vulnerability or potential vulnerability, the Contractor shall cooperate with the Naval Criminal Investigative Service (NCIS), which may include cooperation related to: threat indicators; pre-determined incident information derived from the Contractor's infrastructure systems; and the continuous provision of all Contractor, subcontractor or vendor logs that show network activity, including any additional logs the contractor, subcontractor or vendor agrees to initiate as a result of the cyber incident or notice of actual or potential vulnerability.

5.15.5.2 If the Government determines that the collection of all logs does not adequately protect its interests, the Contractor and NCIS will work together to implement additional measures, which may include allowing the installation of an appropriate network device that is owned and maintained by NCIS, on the Contractor's information systems or information technology assets. The specific details (e.g., type of device, type of data gathered, monitoring period) regarding the installation of an NCIS network device shall be the subject of a separate agreement negotiated between NCIS and the Contractor. In the alternative, the Contractor may install network sensor capabilities or a network monitoring service, either of which must be reviewed for acceptability by NCIS. Use of this alternative approach shall also be the subject of a separate agreement negotiated between NCIS and the Contractor.

5.15.5.3 In all cases, the collection or provision of data and any activities associated with this statement of work shall be in accordance with federal, state, and non-US law.

## 6.0 PLACE OF PERFORMANCE

6.1 The primary place of performance shall be at Contractor's location. However, tasks require support to NSWCPD in the Philadelphia, PA Naval Business Center location; travel to other locations may be required to support assigned tasks.

6.1.1 The Government does not expect Contractor-personnel to sit on-site. If needed on a temporary basis, the Government will make reasonable accommodations to provide space for contractor-personnel under this Task Order, however, no assurances are made.

6.1.2 The specific location(s) will be provided at time of award of the Task Order. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.3 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this Task Order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

#### 6.1.4 Early Dismissal and Closure of Government Facilities

6.1.4.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

6.1.4.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Task Order. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Task Order period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

6.1.5 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing performance at NSWCPD. This document is available at: <https://navsea.navy.deps.mil/wc/pnbc-code10/Safety/default.aspx>

6.1.6 In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by e-mail to (b)(6) (b)(6) that on-site employees have read the "Philadelphia Division Environmental Policy and Commitment" and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD. The e-mail shall include the employee name, work site, and contract number.

### 7.0 TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated number of trips is 50 per year. Travel in support of this requirement is anticipated to include the following alternate performance locations:

CONUS/OCONUS	ORIGIN:	DESTINATION:	Number of Days Per Trip	Number of Trips Per Year	Number of People Per Trip
CONUS	TBD	Norfolk, VA	5	10	2
CONUS	TBD	San Diego, CA	5	10	2
CONUS	TBD	Washington D.C.	5	30	1

7.2 The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR before travel occurs. Approval may be via the Technical Instruction (TI). In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice.

7.3 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002).

#### 7.4 Travel Costs

7.4.1 The current "maximum per diem" rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

### 8.0 GOVERNMENT FURNISHED PROPERTY

Not applicable

### 9.0 GOVERNMENT FURNISHED INFORMATION

Not applicable

### 10.0 PURCHASES

10.1 Only items directly used and incidental to the services for this Task Order and for work within the scope of the Statement of Work, shall be purchased under the Other Direct Cost (ODC) line items. Purchases of an individual item that is valued above \$10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

10.2 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under

this Task Order shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

#### 11.0 COUNTERFEIT MATERIAL PREVENTION

Not applicable

#### 12.0 PERSONNEL

12.1 Personnel Requirements. All persons proposed in key and non-key labor categories shall, at the time of contract award, be U.S. citizens holding at least a current SECRET clearance, or possess a favorable DCSA adjudication as outlined in section 5.3.

12.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state "zero" if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs.

12.3 The level of effort for the performance of the resultant Task Order is based on the following labor categories and hours per year:

Title	eCRAFT Code	Key	GOVT-Site /KR-Site	Hours	Overtime Hours	Resumes Required
Program/Project Manager II	MANP2	Yes	KR	480	0	1
Program/Project Manager I	MANP1	Yes	KR	480	0	1
Engineer, Systems III	ESY3	Yes	KR	1920	96	1
Analyst, Management II	ANM2	Yes	KR	1920	96	1
Systems Administrator IV	SA4	Yes	KR	1920	96	1
Analyst, Management I	ANM1	No	KR	7680	384	0
Logistician I	LGT1	No	KR	3840	192	0
Engineer, Mechanical III	EM3	No	KR	480	24	0
Engineer, Electrical/Electronics III	EE3	No	KR	480	24	0
Engineer, Systems II	ESY2	No	KR	1920	96	0
Specialist, Configuration Management I	SCM1	No	KR	480	24	0
Systems Administrator III	SA3	No	KR	1920	96	0
Security Program Management I	SPM1	No	KR	1920	96	0
Technical Writer, Supervisory	TECW	No	KR	480	24	0
Engineering Technician I	30081	No	KR	480	24	0

#### 12.4 Key Personnel

12.4.1 The Contractor shall allow as many personnel as practicable to remain on the job to help the successor maintain the continuity and consistency of the services required by this Task Order in accordance with Clause 52.237-3 Continuity of Services (Jan 1991) in the basic SeaPort contract. The Contractor also shall disclose necessary personnel records and allow the successor to conduct on-site interviews with these employees. If selected employees are agreeable to the change, the Contractor shall release them at a mutually agreeable date and negotiate transfer of their earned fringe benefits to the successor.

12.4.2 In accordance with C-237-H002 Substitution of Key Personnel, the following labor categories are designated as the Key Personnel for this contract. Resumes will be submitted for each category in the quantities indicated by the key category description. Target or minimum qualifications are listed below for each education and work experience qualifications for each key personnel labor category. The proposed combined expertise of all proposed key personnel shall cover at a minimum all requirements for all task areas in the statement of work.

12.4.3 The Contractor shall provide individuals to fill the key positions identified below.

12.4.4. The Contractor shall indicate within the personnel section of its proposal, and/or indicate within individual submitted resume(s), any personnel security clearance requirements as stipulated in section 12.1 above.

**MANAGER, PROGRAM/PROJECT II** (one (1) resume required):

Target Education: Bachelor's degree from an accredited college or university.

Target Experience: Ten (10) years of combined in-service sustainment program management, Navy ERP financial management, system engineering, technical and shipboard installations/alterations activities-related experience. The Ten (10) years of experience should include experience leading projects that include financial management, planning project/program control, HM&E engineering design, test and evaluation, modifications/alterations, risk management. Working knowledge and direct experience of NSWCPI and NAVSEA SEA21 Programs and Fleet is desired.

**MANAGER, PROGRAM/PROJECT I** (one (1) resume required):

Target Education: Bachelor's degree from an accredited college or university.

Target Experience: Eight (8) years of combined in-service sustainment program management, Navy ERP financial management, system engineering, technical and shipboard installations/alterations activities-related experience. The eight (8) years of experience should include experience leading projects that include financial management, planning project/program control, HM&E engineering design, test and evaluation, modifications/alterations, risk management. Working knowledge and direct experience of NSWCPI and NAVSEA SEA21 Programs and Fleet is desired.

**ENGINEER, SYSTEMS III** (one (1) resume required):

Minimum Education: Bachelor of Science Degree in engineering or Naval Architecture from an accredited college or university.

Target Experience: Seven (7) years of experience in the engineering discipline. This experience should include at least five (5) years leading HM&E engineering efforts and engineering staff involved with the application of engineering disciplines in the technical field directly related HM&E machinery systems onboard USN ships.

**ANALYST, MANAGEMENT II** (one (1) resume required):

Target Education: Bachelor's degree in Business-related discipline from an accredited college or university.

Target Experience: Seven (7) years of experience in the financial, task and overall program management and supporting disciplines. This experience should include at least three (3) years supporting HM&E efforts and systems onboard USN ships.

**SYSTEM ADMINISTRATOR IV** (one (1) resume required):

Target Education: Bachelor's degree in Information Technology from an accredited college or university.

Target Experience: Ten (10) years of experience in information technology and computer programming efforts, including at least three (3) years supporting development of tools for NSWCPI and NAVSEA SEA21 programs.

See Table at 12.6.1 for required certifications.

**12.5 Non-Key Personnel**

12.5.1 In the performance of this effort, the Contractor shall fully staff the non-key positions listed below with qualified individuals. The Contractor shall provide individuals to fill the non-key positions identified below:

**ANALYST, MANAGEMENT I:**

Minimum Education: Bachelor's degree in Engineering or Business from an accredited college or university.

Minimum Experience: Two (2) years of experience in financial and program analysis; budgeting, scheduling, planning, estimating, and progress of program management/programmatic plans in support of engineering systems. Shall have relative experience to HM&E and SEA21 programs.

**LOGISTICIAN I:**

Minimum Education: Bachelor's degree in Engineering or Business from an accredited college or university.

Minimum Experience: Two (2) years of experience in supply chain analysis; provisioning, budgeting, scheduling, planning, estimating, and progress of program management/programmatic plans in support of engineering systems. Shall have relative experience to HM&E and SEA21 programs.

### **ENGINEER, MECHANICAL III:**

Minimum Education: Bachelor's degree in Engineering from an accredited college or university.

Minimum Experience: Seven (7) years of experience in the engineering discipline, of which at least five (5) years shall include leading HM&E engineering efforts engineering staff involved with the application of engineering disciplines in the technical field directly related HM&E machinery systems onboard USN ships.

### **ENGINEER, ELECTRICAL/ELECTRONICS III:**

Minimum Education: Bachelor's degree in Engineering from an accredited college or university.

Minimum Experience: Seven (7) years of experience in the engineering discipline, of which at least five (5) years shall include leading HM&E engineering efforts engineering staff involved with the application of engineering disciplines in the technical field directly related HM&E machinery systems onboard USN ships.

### **ENGINEER, SYSTEMS II**

Minimum Education: Bachelor's degree in Engineering from an accredited college or university.

Minimum Experience: Three (3) years of experience in the engineering discipline, demonstrating experience integrating various network operating systems, application programs and hardware devices.

### **SPECIALIST, CONFIGURATION MGMT I**

Minimum Education: Bachelor's degree from an accredited college or university.

Minimum Experience: Two (2) years of experience of program management/programmatic plans in support of engineering systems. Shall have relative experience to HM&E and SEA21 programs.

### **SYSTEMS ADMINISTRATOR III**

Minimum Education: Bachelor's degree in Engineering, Computer Science, or Information Systems from an accredited college or university.

Minimum Experience: Seven (7) years of experience in the engineering, computer science, and/or information systems discipline, demonstrating experience supporting operational requirements of computer network systems including workstation, file servers, and web servers.

See Table at 12.6.1 for required certifications.

### **SECURITY PROGRAM MANAGEMENT I**

Minimum Education: Associate Degree from accredited University or CNSSI 4011 Certificate or AQD GA7

Minimum Experience: Two (2) years of experience of program management/programmatic plans in support of engineering systems. Shall have relative experience to HM&E and SEA21 programs.

See Table at 12.6.1 for required certifications.

### **TECHNICAL WRITER, SUPERVISORY**

Minimum Education: Bachelor's degree in any field from accredited college or university.

Minimum Experience: Three (3) years of experience developing, writing and editing material for reports, manuals, briefs, proposals, instructions books, catalogs and related publications.

## ENGINEERING TECHNICIAN I

Minimum Education: High school graduate or GED; graduate of a military school that provided an in-depth knowledge of naval shipboard systems maintenance and operation; or be a graduate of a trade, industrial or correspondence school for engineering.

Minimum Experience: One (1) year of experience assembling or installing equipment or parts requiring simple wiring, soldering, or connecting; performing simple or routine tasks or tests such as tensile or hardness tests; operating and adjusting simple test equipment; records test data; gathering and maintaining specified records of engineering data such as tests, drawings, performing computations by substituting numbers in specified formulas; or plotting data and draws simple curves and graphs.

### 12.6 DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program contractors performing IA functions must be designated as a member of the Cybersecurity/IA Workforce and meet qualification requirements for their duties, which may include both an IA baseline certification and operating system (OS)/Computing Environment (CE) certification requirement per below instructions:

1. Contractors performing Cybersecurity/IA functions must meet the minimum IA baseline certification prior to being engaged as defined in the CSWF Matrix below.
2. Contractor personnel agree as a "condition of employment" to obtain (and maintain) the appropriate certifications and continuing profession education requirements for Cybersecurity/IAWF position.
3. Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570.01-M. The contractor is responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570.01-M and the Computing Environment/Operating System (CE/OS) certifications in accordance with the CSWF Matrix below.
4. Upon hire all contractor personnel assigned to the IAM/IAT Level I-III position (as appropriate) shall sign the Information System Privileged Access Agreement Acknowledgement of Responsibilities statement.

Cybersecurity/IA Workforce labor categories are identified herein. The Contractor shall ensure that personnel have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including:

1. DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
2. Appropriate operating system certification for information assurance technical (IAT) positions as required by DoD 8570.01-M.
3. The Contractor shall provide the current information assurance certificates/documentation supporting IA certification and current status of personnel performing Cybersecurity/IA duties. Baseline and Operating System (OS) Certification requirements listed in the CSWF Matrix must be met and are a condition of hire.



4. The contractor shall ensure that cybersecurity/IA contractor personnel are appropriately certified and maintain current Continuing Professional Education (CPE) requirement as a condition of employment.

5. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

**Information assurance contractor training and certification:**

1. This contract includes information assurance functional services for DoD information systems, and requires appropriately cleared contractor personnel to access information system to perform contract duties, the contractor is responsible for providing to the contracting officer-

a. A list of information assurance functional responsibilities for DoD information systems by category (e.g., technical or management) and level (e.g., computing network environment, or enclave); and

b. The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information functional responsibilities.

2. After contract award, the contractor is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented and tracked.

3. The responsibilities specified apply to all DoD information assurance duties supported by a contractor, whether performed full-time or part-time as additional or emergency duties, and when using a DoD contract, or a contract or agreement administered by another agency.

**Baseline Certification-** The baseline certification is a security certification and is required for all IA members (all IAT and IAM levels) of the Cybersecurity Workforce/IA Workforce. Contractors must have a baseline certification prior to performing any IA duties and is a condition of hire.

**Computing Environment (CE) Certification-** All IAT levels require Computing Environment certification for the appropriate operating system they support and in which access is granted. These certifications are typically vendor specific and depend on the supported hardware or operating system. (i.e., Microsoft computing environment requires MCITP-SA and Linux computing environment requires LINUX+).

**Continuing Professional Education (CPE) Requirements-** As technology continuously advances; nearly all certifications expire or have continuing professional education (CPE) requirements. Both the baseline certifications and computing environment certifications may require continuous education. The vendor requirements state whether the certifications require continuous education.

1. Continuing Professional Education (CPE) requirements are not a direct contractor cost to the Government. The contractor is responsible for meeting the qualification requirements for all positions on the contract in the Cybersecurity/IAWF matrix and should not invoice the Government for training, certification tests, or continuing professional education requirements.

**Information Assurance Functions and Personnel Requirements Note:**

Ensure that if you have any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS)

workforce you must identify the required security, certifications, education, and training for EACH labor category. Reference DFARS Clause 252.239-7001, DoD 8750.01-M "Information Workforce Improvement Program", and DoD 8140.01 "Cyberspace Workforce Management".

12.6.1 Contractor shall ensure that employees keep all required certifications current to meet Navy Information Assurance (IA) Workforce requirements. The table below outlines the requirements for the listed cyber positions:

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System/Computing Environment(OS/CE) Qualification	Primary Tasks
				I	I	I
Systems Administrator IV	45	Advanced	IAT-3	CASP+ CE CCNP Security CISA CISSP (or Associate) GCED GCIH	Directed by Privileged Access Agreement	3 0
Systems Administrator III	45	Intermediate	IAT-2	CCNA Security CySA+ ** GICSP GSEC Security+ CE SSCP	Directed by Privileged Access Agreement	3 0
Security Program Management I	72	Basic	IAM-1	CAP CND Cloud+ GSLC Security+ CE	Directed by Privileged Access Agreement	3 0

### 13.0 NSWCPD ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (ECRAFT) SYSTEM

13.1 In addition to the requirements of Clause C-237-W001 "Electronic Cost Reporting and Financial Tracking (eCRAFT) System Reporting (NAVSEA)", the contractor is required to provide supporting accounting system reports, at the Contracting Officer's request, based on the review of the invoice documentation submitted to eCRAFT. This documentation will include reports such as the Job Summary Report (or equivalent), Labor Distribution Report (or equivalent), and General Ledger Detail Report (or equivalent). Supporting labor data provided must include unburdened direct labor rates for each employee and labor category. Cost breakdowns for ODCs, Materials, travel and other non-labor costs must be at the transactional level in sufficient detail so the Government can review allocability to the Task Order. Indirect costs allocated to direct costs must be shown at the lowest level of detail sufficient to reconcile each indirect rate to the appropriate allocation base.

13.2 On invoices containing subcontractor costs, the prime contractor agrees, at the Contracting Officer's request, to attach as supporting documentation all invoices received from subcontractors, unless the subcontractor submits invoices directly to the CO and COR. This requirement applies to all subcontract types (Cost, FFP, etc.).

#### 14.0 SPECIAL REQUIREMENTS

Not applicable

#### C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nine num characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number.

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plus the applicable nine-position NIIN assigned to the item of supply.

(End of Text)

#### C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as "protected information". File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that:

(1) The support contractor not disclose any information;

(2) Individual employees are to be instructed by the support contractor regarding the sensitivity of the official contract files;

(3) The support contractor performing these services be barred from providing any other supplies and/or services, or competing to do so, to NAVSEA for the period of performance of its contract and for an additional three years thereafter unless otherwise provided by law or regulation; and,

(4) In addition to any other rights the contractor may have, it is a third party beneficiary who has the right of direct action against the support contractor, or any person to whom the support contractor has released or disclosed protected information, for the unauthorized duplication, release, or disclosure of such protected information.

(c) Execution of this contract by the contractor is considered consent to NAVSEA's permitting access to any information, irrespective of restrictive markings or the nature of the information submitted, by its file room management support contractor for the limited purpose of executing its file room support contract responsibilities.

(d) NAVSEA may, without further notice, enter into contracts with other contractors for these services. Contractors should enter into separate non-disclosure agreements with the file room contractor. Contact the Procuring Contracting Officer for contractor specifics. However, any such agreement will not be considered a prerequisite before information submitted is stored in the file room or otherwise encumber the government.

(End of Text)

#### C-211-H001 ACCESS TO THE VESSEL(S) (NAVSEA) (OCT 2018)

Officers, employees and associates of other prime Contractors with the Government and their subcontractors, shall, as authorized by the Supervisor, have, at all reasonable times, admission to the plant, access to the vessel(s) where and as required, and be permitted, within the plant and on the vessel(s) required, to perform and fulfill their respective obligations to the Government. The Contractor shall make reasonable arrangements with the Government or Contractors of the Government, as shall have been

identified and authorized by the Supervisor to be given admission to the plant and access to the vessel(s) for office space, work areas, storage or shop areas, or other facilities and services, necessary for the performance of the respective responsibilities involved, and reasonable to their performance.

(End of Text)

#### **C-211-H016 SPECIFICATIONS AND STANDARDS (NAVSEA) (OCT 2018)**

(a) Definitions.

(i) A "zero-tier reference" is a specification, standard, or drawing that is cited in the contract (including its attachments).

(ii) A "first-tier reference" is either: (1) a specification, standard, or drawing cited in a zero-tier reference, or (2) a specification cited in a first-tier drawing.

(b) Requirements. All zero-tier and first-tier references, as defined above, are mandatory for use. All lower tier references shall be used for guidance only unless specifically identified below.

NONE

(End of Text)

#### **C-211-H017 UPDATING SPECIFICATIONS AND STANDARDS (NAVSEA) (DEC 2018)**

The contractor may request that this contract be updated to include the current version of the applicable specification or standard if the update does not affect the form, fit or function of any deliverable item or increase the cost/price of the item to the Government. The contractor should submit update requests to the Procuring Contracting Officer with copies to the Administrative Contracting Officer and cognizant program office representative for approval. The contractor shall perform the contract in accordance with the existing specifications and standards until notified of approval/disapproval of its request to update by the Procuring Contracting Officer. Any approved alternate specifications or standards will be incorporated into the contract.

(End of Text)

#### **C-211-H018 APPROVAL BY THE GOVERNMENT (NAVSEA) (JAN 2019)**

Approval by the Government as required under this contract and applicable specifications shall not relieve the Contractor of its obligation to comply with the specifications and with all other requirements of the contract, nor shall it impose upon the Government any liability it would not have had in the absence of such approval.

(End of Text)

#### **C-215-H002 CONTRACTOR PROPOSAL (NAVSEA) (OCT 2018)**

(a) Performance of this contract by the Contractor shall be conducted and performed in accordance with detailed obligations to which the Contractor committed itself in Proposal M-20-39 dated 09 September 2020 in response to NAVSEA Solicitation No. N6449820R3012.

(b) The technical volume(s) of the Contractor's proposal is(are) hereby incorporated by reference and made subject to the "Order of Precedence" (FAR 52.215-8) clause of this contract. Under the "Order of Precedence" clause, the technical volume(s) of the Contractor's proposal referenced herein is (are) hereby designated as item (f) of the clause, following "the specifications" in the order of precedence.

(End of Text)

#### **C-222-H001 ACCESS TO THE VESSELS BY NON-U.S. CITIZENS (NAVSEA) (APR 2019)**

(a) No person not known to be a U.S. citizen shall be eligible for access to naval vessels, work sites and adjacent areas when said vessels are under construction, conversion, overhaul, or repair, except upon a finding by COMNAVSEA or his designated representative that such access should be permitted in the best interest of the United States. The Contractor shall establish procedures to comply with this requirement and NAVSEAINST 5510.2D.

(b) If the Contractor desires to employ non-U.S. citizens in the performance of work under this contract or agreement that requires access as specified in paragraph (a) of this requirement, approval must be obtained prior to access for each contract or agreement where such access is required. To request such approval for non-U.S. citizens of friendly countries, the Contractor shall submit to the cognizant Contract Administration Office (CAO), an Access Control Plan (ACP) which shall contain as a minimum, the following information:

(1) Badge or Pass oriented identification, access, and movement control system for non-U.S. citizen employees with the badge or pass to be worn or displayed on outer garments at all times while on the Contractor's facilities and when performing work aboard ship.

(i) Badges must be of such design and appearance that permits easy recognition to facilitate quick and positive identification.

- (ii) Access authorization and limitations for the bearer must be clearly established and in accordance with applicable security regulations and instructions.
- (iii) A control system, which provides rigid accountability procedures for handling lost, damaged, forgotten or no longer required badges, must be established.
- (iv) A badge or pass check must be performed at all points of entry to the Contractor's facilities or by a site supervisor for work performed on vessels outside the Contractor's plant.
- (2) Contractor's plan for ascertaining citizenship and for screening employees for security risk.
- (3) Data reflecting the number, nationality, and positions held by non-U.S. citizen employees, including procedures to update data as non-U.S. citizen employee data changes, and pass to cognizant CAO
- (4) Contractor's plan for ensuring subcontractor compliance with the provisions of the Contractor's ACP.
- (5) These conditions and controls are intended to serve as guidelines representing the minimum requirements of an acceptable ACP. They are not meant to restrict the Contractor in any way from imposing additional controls necessary to tailor these requirements to a specific facility.
- (c) To request approval for non-U.S. citizens of hostile and/or communist-controlled countries (listed in Department of Defense Industrial Security Manual, DOD 5220.22-M or available from cognizant CAO), Contractor shall include in the ACP the following employee data: name, place of birth, citizenship (if different from place of birth), date of entry to U.S., extenuating circumstances (if any) concerning immigration to U.S., number of years employed by Contractor, position, and stated intent concerning U.S. citizenship. COMNAVSEA or his designated representative will make individual determinations for desirability of access for the above group. Approval of ACPs for access of non-U.S. citizens of friendly countries will not be delayed for approval of non-U.S. citizens of hostile communist-controlled countries. Until approval is received, Contractor must deny access to vessels for employees who are non-U.S. citizens of hostile and/or communist-controlled countries.
- (d) The Contractor shall fully comply with approved ACPs. Noncompliance by the Contractor or subcontractor serves to cancel any authorization previously granted, in which case the Contractor shall be precluded from the continued use of non-U.S. citizens on this contract or agreement until such time as the compliance with an approved ACP is demonstrated and upon a determination by the CAO that the Government's interests are protected. Further, the Government reserves the right to cancel previously granted authority when such cancellation is determined to be in the Government's best interest. Use of non-U.S. citizens, without an approved ACP or when a previous authorization has been canceled, will be considered a violation of security regulations. Upon confirmation by the CAO of such violation, this contract, agreement or any job order issued under this agreement may be terminated for default in accordance with the clause entitled "Default (Fixed-Price Supply And Service)" (FAR 52.249-8), "Default (Fixed-Price Research And Development)" (FAR 52.249-9) or "Termination (Cost Reimbursement)" (FAR 52.249-6), as applicable.
- (e) Prime Contractors have full responsibility for the proper administration of the approved ACP for all work performed under this contract or agreement, regardless of the location of the vessel, and must ensure compliance by all subcontractors, technical representatives and other persons granted access to U.S. Navy vessels, adjacent areas, and work sites.
- (f) In the event the Contractor does not intend to employ non-U.S. citizens in the performance of the work under this contract, but has non-U.S. citizen employees, such employees must be precluded from access to the vessel and its work site and those shops where work on the vessel's equipment is being performed. The ACP must spell out how non-U.S. citizens are excluded from access to contract work areas.
- (g) The same restriction as in paragraph (f) above applies to other non-U.S. citizens who have access to the Contractor's facilities (e.g., for accomplishing facility improvements, from foreign crewed vessels within its facility, etc.) except that, with respect to access to the vessel and worksite, the restrictions shall not apply to uniformed U.S. Navy personnel who are non-U.S. citizens and who are either assigned to the ship or require access to the ship to perform their duties.

(End of Text)

#### **C-223-W002 ON-SITE SAFETY REQUIREMENTS (NAVSEA) (OCT 2018)**

- (a) The contractor shall ensure that each contractor employee reads any necessary safety documents within 30 days of commencing performance at any Government facility. Required safety documents can be obtained from the respective safety office. Contractors shall notify the Safety office points of contact below to report completion of the required training via email. The email shall include the contractor employee's name, work site, and contract number.
- (b) It is expected that contractor employees will have received training from their employer on hazards associated with the areas in which they will be working and know what to do in order to protect themselves. Contractors are required to adhere to the requirements of 29 CFR 1910, 29 CFR 1926 and applicable state and local requirements while in Government spaces. The contractor shall ensure that all on-site contractor work at the Government facility is in accordance with any local safety instructions as provided via the COR. The contractor shall report all work-related injuries/illnesses that occurred while working at the Government site to the COR.
- (c) Contractors whose employees perform work within Government spaces in excess of 1000 hours per calendar quarter during a calendar year shall submit the data elements on OSHA Form 300A, Summary of Work Related Injuries and Illnesses, for those employees to the safety office, via the COR by 15 January for the previous calendar year, even if no work related injuries or illnesses occurred. If a contractor's injury/illness rates are above the Bureau of Labor Statistics industry standards, a safety assessment may be performed by the Safety Office to determine if any administrative or engineering controls can be utilized to prevent further injuries/illnesses, or if any additional Personal Protective Equipment or training will be required.
- (d) Any contractor employee exhibiting unsafe behavior may be removed from the Government site. Such removal shall not relieve the contractor from meeting its contractual obligations and shall not be considered an excusable delay as defined in FAR 52.249-14.

(End of Text)

**C-227-H006 DATA REQUIREMENTS (NAVSEA) (OCT 2018)**

The data to be furnished hereunder shall be prepared in accordance with the Contract Data Requirements List, DD Form 1423, and Exhibit(s) A001-A008, attached hereto.

A001 – Contract Status Report

A002 – Travel Trip Report

A003 – Contractor Personnel Roster

A004 – Small Business Utilization

A005 – Systems Security Plan

A006 – Funds Status Report

A007 – Computer Software Product

A008 – Technical Report Study/Services

(End of Text)

**C-227-H008 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (NAVSEA) (DEC 2018)**

(a) The contractor shall actively participate in the Government Industry Data Exchange Program in accordance with the GIDEP Operations Manual, S0300-BT-PRO-010. The contractor shall submit information concerning critical or major nonconformances, as defined in FAR 46.407/DFARS 246.407, to the GIDEP information system.

(b) The contractor shall insert paragraph (a) of this clause in any subcontract when deemed necessary. When so inserted, the word "contractor" shall be changed to "subcontractor."

(c) The contractor shall, when it elects not to insert paragraph (a) in a subcontract, provide the subcontractor any GIDEP data which may be pertinent to items of its manufacture and verify that the subcontractor utilizes any such data.

(d) The contractor shall, whether it elects to insert paragraph (a) in a subcontract or not, verify that the subcontractor utilizes and provides feedback on any GIDEP data that may be pertinent to items of its manufacture."

(e) GIDEP materials, software and information are available without charge from:

GIDEP Operations Center

P.O. Box 8000

Corona, CA 92878-8000

Phone: (951) 898-3207

FAX: (951) 898-3250

Internet: <http://www.gidep.org>

(End of Text)

**C-227-H013 REPORTING THE INTENDED USE OF GOVERNMENT-UNIQUE MARKS (NAVSEA) (JAN 2020)**

(a) Government-unique mark, as used herein, means any mark that identifies and distinguishes goods first developed or manufactured in performance of a Government contract or that identifies and distinguishes services first rendered in performance of a Government contract.

(b) The Contractor must notify the Contracting Officer in writing of its intent to assert rights in, or file an application to register, a Government-unique mark. The Contractor's notification shall be in writing and shall identify the Government-unique mark (including the word, name, symbol, or design), provide a statement as to its intended use(s) in commerce, and list the particular classes of goods or services in which registration will be sought.

(c) Failure of the Government to respond to the notification does not waive the Government's right under the Trademark Act to contest the Contractor's assertion of rights or application.

(d) Nothing contained herein provides authorization or consent, express or implied, by the Government regarding the Contractor's use of any mark, including a Government-unique mark.

(End of Text)

#### **C-237-H001 SERVICE CONTRACT REPORTING (NAVSEA) (JAN 2021)**

(a) Services Contract Reporting (SCR) requirements apply to this contract. The contractor shall report required SCR data fields using the SCR section of the System for Award Management (SAM) at following web address: <https://sam.gov/SAM/>.

(b) Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at <https://sam.gov/SAM/>.

(End of Text)

#### **C-237-H002 SUBSTITUTION OF KEY PERSONNEL (NAVSEA) (OCT 2018)**

(a) The Contractor agrees that a partial basis for award of this contract is the list of key personnel proposed. Accordingly, the Contractor agrees to assign to this contract those key persons whose resumes were submitted with the proposal necessary to fulfill the requirements of the contract. No substitution shall be made without prior notification to and concurrence of the Contracting Officer in accordance with this requirement. Substitution shall include, but not be limited to, subdividing hours of any key personnel and assigning or allocating those hours to another individual not approved as key personnel.

(b) All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Contracting Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include: (1) an explanation of the circumstances necessitating the substitution; (2) a complete resume of the proposed substitute; (3) an explanation as to why the proposed substitute is considered to have equal or better qualifications than the person being replaced; (4) payroll record of the proposed replacement; and (5) any other information requested by the Contracting Officer to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

(c) Key personnel are identified in an attachment in Section J.

(End of Text)

#### **C-237-W001 ELECTRONIC COST REPORTING AND FINANCIAL TRACKING (eCRAFT) SYSTEM REPORTING (NAVSEA) (MAY 2019)**

(a) The Contractor agrees to upload the Contractor's Funds and Man-hour Expenditure Reports in the Electronic Cost Reporting and Financial Tracking (eCRAFT) System and submit the Contractor's Performance Report on the day and for the same timeframe the contractor submits an invoice into the Wide Area Workflow (WAWF) module on the Procurement Integrated Enterprise Environment (PIEE) system. Compliance with this requirement is a material requirement of this contract. Failure to comply with this requirement may result in contract termination.

(b) The Contract Status Report indicates the progress of work and the status of the program and of all assigned tasks. It informs the Government of existing or potential problem areas.

(c) The Contractor's Fund and Man-hour Expenditure Report reports contractor expenditures for labor, materials, travel, subcontractor usage, and other contract charges.

(1) Access: : eCRAFT: Reports are uploaded through the eCRAFT System Periodic Report Utility (EPRU). The EPRU spreadsheet and user manual can be obtained at: <http://www.navsea.navy.mil/Home/Warfare-Centers/NUWC-Newport/Partnerships/Commercial-Contracts/Information-eCraft/> under eCRAFT information. The link for eCRAFT report submission is: [https://www.pdrep.csd.disa.mil/pdrep\\_files/other/ecraft.htm](https://www.pdrep.csd.disa.mil/pdrep_files/other/ecraft.htm). If you have problems uploading reports, please see the Frequently Asked Questions at the site address above.

(2) Submission and Acceptance/Rejection: Submission and Acceptance/Rejection: The contractor shall submit their reports on the same day and for the same timeframe the contractor submits an invoice in WAWF. The amounts shall be the same. eCRAFT acceptance/rejection will be indicated by e-mail notification from eCRAFT.

(End of Text)

#### **C-242-H001 EXPEDITING CONTRACT CLOSEOUT (NAVSEA) (OCT 2018)**

(a) As part of the negotiated fixed price or total estimated amount of this contract, both the Government and the Contractor have agreed to waive any entitlement that otherwise might accrue to either party in any residual dollar amount of \$1,000 or less at the time of final contract closeout. The term "residual dollar amount" shall include all money that would otherwise be owed to either party at the end of the contract, except that, amounts connected in any way with taxation, allegations of fraud and/or antitrust violations shall be excluded. For purposes of determining residual dollar amounts, offsets of money owed by one party against money that would otherwise be paid by that party may be considered to the extent permitted by law.

(b) This agreement to waive entitlement to residual dollar amounts has been considered by both parties. It is agreed that the administrative costs for either party associated

with collecting such small dollar amounts could exceed the amount to be recovered.

(End of Text)

#### **C-242-H002 POST AWARD MEETING (NAVSEA) (OCT 2018)**

(a) A post-award meeting with the successful offeror will be conducted within [ \* ] days after award of the [contract / task order]. The meeting will be held at the address below:

Location/Address: via teleconference

(b) The contractor will be given [ \* ] working days notice prior to the date of the meeting by the Contracting Officer.

(c) The requirement for a post-award meeting shall in no event constitute grounds for excusable delay by the contractor in performance of any provisions in the [contract / task order].

(d) The post-award meeting will include, but is not limited to, the establishment of work level points of contact, determining the administration strategy, roles and responsibilities, and ensure prompt payment and close out. Specific topics shall be mutually agreed to prior to the meeting.

[ \* ] To be specified at [contract / task order] award

(End of Text)

#### **C-242-H003 TECHNICAL INSTRUCTIONS (NAVSEA) (OCT 2018)**

(a) Performance of the work hereunder may be subject to written technical instructions signed by the Contracting Officer and the Contracting Officer's Representative specified in Section G of this contract. As used herein, technical instructions are defined to include the following:

(1) Directions to the Contractor which suggest pursuit of certain lines of inquiry, shift work emphasis, fill in details or otherwise serve to accomplish the contractual statement of work.

(2) Guidelines to the Contractor which assist in the interpretation of drawings, specifications or technical portions of work description.

(b) Technical instructions must be within the general scope of work stated in the contract. Technical instructions may not be used to: (1) assign additional work under the contract; (2) direct a change as defined in the "CHANGES" clause of this contract; (3) increase or decrease the contract price or estimated contract amount (including fee), as applicable, the level of effort, or the time required for contract performance; or (4) change any of the terms, conditions or specifications of the contract.

(c) If, in the opinion of the Contractor, any technical instruction calls for effort outside the scope of the contract or is inconsistent with this requirement, the Contractor shall notify the Contracting Officer in writing within ten (10) working days after the receipt of any such instruction. The Contractor shall not proceed with the work affected by the technical instruction unless and until the Contractor is notified by the Contracting Officer that the technical instruction is within the scope of this contract.

(d) Nothing in the foregoing paragraph shall be construed to excuse the Contractor from performing that portion of the contractual work statement which is not affected by the disputed technical instruction.

(End of Text)

#### **C-244-H002 SUBCONTRACTORS/CONSULTANTS (NAVSEA) (OCT 2018)**

Notwithstanding FAR 52.244-2(d) and in addition to the information required by FAR 52.244-2(e) of the contract, the contractor shall include the following information in requests to add subcontractors or consultants during performance, regardless of subcontract type or pricing arrangement:

(1) Impact on subcontracting goals,

(2) Impact on providing support at the contracted value,

(3) The results of negotiations to incorporate fee rate caps no higher than the lower of (i) SeaPort-e fee rate caps for the prime contractor, or in the case where the proposed subcontractor is also a SeaPort-e prime, (ii) fee rate caps that are no higher than the subcontractor's prime SeaPort-e contract.

(End of Text)

#### **C-245-H005 INFORMATION AND DATA FURNISHED BY THE GOVERNMENT--ALTERNATE I (NAVSEA) (MAY 2019)**

(a) Contract Specifications, Drawings and Data. The Government will furnish, if not included as an attachment to the contract, any unique contract specifications or other design or alteration data cited or referenced in Section C.



(b) Government Furnished Information (GFI). GFI is defined as that information essential for the installation, test, operation, and interface support of all Government Furnished Material identified in an attachment in Section J. The Government shall furnish only the GFI identified in an attachment in Section J. The GFI furnished to the contractor need not be in any particular format. Further, the Government reserves the right to revise the listing of GFI as follows:

(1) The Contracting Officer may at any time by written order:

- (i) delete, supersede, or revise, in whole or in part, data identified in an attachment in Section J; or
- (ii) add items of data or information to the attachment identified in Section J; or
- (iii) establish or revise due dates for items of data or information in the attachment identified in Section J.

(2) If any action taken by the Contracting Officer pursuant to subparagraph (1) immediately above causes an increase or decrease in the costs of, or the time required for, performance of any part of the work under this contract, the contractor may be entitled to an equitable adjustment in the contract amount and delivery schedule in accordance with the procedures provided for in the "CHANGES" clause of this contract.

(c) Except for the Government information and data specified by paragraphs (a) and (b) above, the Government will not be obligated to furnish the Contractor any specification, standard, drawing, technical documentation, or other publication, notwithstanding anything to the contrary in the contract specifications, the GFI identified in an attachment in Section J, the clause of this contract entitled "Government Property" (FAR 52.245-1) or "Government Property Installation Operation Services" (FAR 52.245-2), as applicable, or any other term or condition of this contract. Such referenced documentation may be obtained:

- (1) From the ASSIST database via the internet at <https://assist.dla.mil/online/start/>; or
- (2) By submitting a request to the

Department of Defense Single Stock Point (DoDSSP)

Building 4, Section D

700 Robbins Avenue

Philadelphia, Pennsylvania 19111-5094

Telephone (215) 697-6396

Facsimile (215) 697-9398

Commercial specifications and standards, which may be referenced in the contract specification or any sub-tier specification or standard, are not available from Government sources and should be obtained from the publishers.

(End of Text)

#### **C-247-H001 PERMITS AND RESPONSIBILITIES (NAVSEA) (DEC 2018)**

The Contractor shall, without additional expense to the Government, be responsible for obtaining any necessary licenses and permits for complying with any applicable Federal, State, and Municipal laws, codes, and regulations for shipping and transportation including, but not limited to, any movement over public highways of overweight/over dimensional materials.

(End of Text)